논문

블록체인 기술을 활용한 진본인증 모형 연구*

A Study on Authentication Model using Blockchain

이경남(Lee, Kyung-nam)**

1. 서론
2. 블록체인 기술의 이해
   1) 블록체인의 구조
   2) 주요 개념
3. 진본인증을 위한 블록체인 기술 적용가능성
   1) 진본인증 개념
   2) 진본인증을 위한 블록체인 기술 활용
4. 기록관리를 위한 블록체인 모형 설계
   1) 기록관리를 위한 블록체인 개념 설계
   2) 기록관리를 위한 블록체인 모형 제안
   3) 기록관리 거버넌스 기대효과
5. 결론

* 본 논문은 저자의 한국외국어대학교 정보·기록학과 박사학위논문(2018)의 일부를 수정·보완한 것임.

** 한국외국어대학교 정보·기록학과 박사(coarchivist@gmail.com).

■투고일 : 2019년 1월 1일 ■최초심사일 : 2019년 1월 3일 ■게재확정일 : 2019년 1월 14일.

〈초록〉

디지털 기술의 급속한 변화에 따라 전자기록의 장기보존 체계를 확립하기 위해 새로운 패러다임으로의 전환이 필요한 시점이다. 본 연구는 기록관리를 위한 새로운 기술의 적용가능성을 모색해보기 위해 블록체인 기술의 기록관리 적용가능성을 탐색해보고, 기록관리를 위한 모형 개발을 목적으로 한다. 블록체인에 대한 개념적 분석과 기록관리 프로세스를 고려하여 기록의 진본 인증에 적합한 블록체인 모형을 제안하였다. 이를 위해 블록체인 네트워크의 구성과 블록의 구조, 합의 알고리즘을 설계하고 블록체인 모형을 제안하였으며, 블록체인을 기록관리에 적용함으로써 기관 간 수평적 협력체계를 구현하는 거버넌스 측면의 변화를 예측하였다.

주제어 : 전자기록관리, 진본인증, 진본성, 블록체인, 분산원장, 거버넌스

〈Abstract〉

With the rapid changes in the digital technology, it is necessary to shift to a new paradigm corresponding to the changing environment was recognized. This study actively explores the possibility of applying new technologies for recordkeeping. This study aimed to investigate the applicability of blockchain to recordkeeping and to develop a new model for recordkeeping based on it. Through a conceptual analysis of blockchain and consideration of the recordkeeping process, a blockchain model that is suitable for the authentication of records was proposed. For this the network structure, the structure of blockchain blocks, a consensus algorithm, and recordkeeping blockchain model were designed. It also predicted potential changes in digital records management when applying blockchain. It predicted change in governance aspects to implement a horizontal cooperation system among the archives.

Keywords : digital records management, authentication, authenticity, blockchain, distributed ledger, governance

1. 서론

디지털 산업의 급변하는 기술적 환경은 디지털 혁명으로 일컬어지며 산업, 정부, 사회 전반에 큰 변화를 가져올 뿐만 아니라, 개인의 삶의 방식에도 영향을 줄 것으로 전망된다. 이러한 기술 변화는 이전의 산업혁명과 그 속도와 범위에서 기하급수적 차이를 보이고, 그 변화의 폭과 깊이 역시 산업 전반의 생산, 관리, 거버넌스 시스템의 변화를 초래하므로 제4차 산업혁명으로 보는 견해가(Klaus Schwab 2016) 지지를 얻고 있으며, 이에 대한 활발한 논의가 전 세계적으로 이루어지고 있다.

급속한 변화의 조류 속에서 선진 기술의 추격에 급급한 기존의 연구개발 방식에서 탈피하여, 새로운 기술의 적용가능성을 다양한 관점에서 모색해 보고 근본적이고 종합적인 분석과 대응 체계를 갖추어야 한다. 특히 전자기록의 비중이 높은 국내의 공공기록관리 분야는 디지털 환경 변화에 민감하게 대응해야 할 필요가 있다. 전자기록을 둘러싼 디지털 환경의 분석과 기술 동향의 변화를 주시해야 한다. 전자기록관리 환경도 제4차 산업혁명으로 대변되는 기술적 변화에 직면하여, 전자기록의 생산과 관리, 보존 환경이 영향을 받고 있다.

단계적이고 계층적인 기존의 기록관리 체계에서 벗어나 정보 거버넌스 관점으로의 전환이 필요하다고 생각된다. 기존의 종이문서 기반의 기록관리 체계가 현재의 전자기록관리 환경에 적합하지 않다는 것이 지적되고 있다. 정보통신기술의 변화에 따라 업무 환경이 변하고, 이러한 변화는 생산되는 기록의 유형과 기록을 관리하는 방식의 변화를 수반한다. 단계적이고 계층적인 기존의 기록관리 체계를 재검토하여 협업과 통합을 바탕으로 한 이음새 없는(seamless) 프로세스로 전환할 필요가 있다. 기록관리 기관간의 수평적 관계로 나아가는 거버넌스 관점의 패러다임 전환이 요구되는 시점이다.

기록관리의 핵심은 생산과정에 대한 신뢰성과 관리과정의 무결성, 그리

고 신뢰성과 무결성으로 입증되는 진본성을 유지하는 것이라 할 수 있다. 이 연구에서는 기록이 생산된 바 그대로의 목적을 유지하기 위해 진본성을 보장하는 방안으로 제4차 산업혁명의 주요 기술로 주목받고 있는 블록체인 기술의 적용가능성을 검토해보고자 한다. 기록관리학 관점에서 블록체인 기술을 이해하고, 적용하기 위한 개념 모델 제안을 연구의 목적으로 한다. 블록체인 기술의 기록관리 적용 방안을 검토함으로써 기술변화에 조응하는 기록관리 체계 마련을 위한 단초를 제공해보고자 한다.

블록체인 기술에 대한 선행연구는 핀테크 분야에서 시작되어 점차 공공 영역으로 확산되고 있으며, 북미 지역과 유럽, 호주를 비롯한 여러 나라에서 국가적 지원을 바탕으로 연구 개발을 정책적으로 주도하고 있다. 자산관리를 비롯하여 워크플로우 관리, 디지털 권한관리, 투표, 세금, 증명서 발급, 공증, 신원확인 서비스 등의 다양한 분야에서 활용하기 위한 시도들이 이어지고 있다.

기록관리와 관련한 연구로는 캐나다의 브리티시 컬럼비아 대학의 Blockchain 프로젝트[1]를 주목할 만하다. 블록체인 기술의 적용 사례 연구와 블록체인 기술 분석, 기록관리 분야의 적용가능성에 대해 산학협력체계를 구축하여 연구를 진행하고 있다. 이 외에도 블록체인을 기록관리에 적용하기 위한 실험연구가 진행되고 있는데 미국 보건정보기술국의 의료 기록 관리[2] 및 영국 법무부의 디지털 수사 증거 관리[3], 두바이의 전자문서 시스템 구축[4] 등의 시범사업 등이 있다. 그러나 이러한 연구 프로젝트들이 시작되는 단계이므로 향후 상용화 보급을 위해서는 연구 성과들을 지켜볼 필요가 있다.

---

1) Blockchain@UBC 〈https://blockchainubc.ca〉
2) Laure A. Linn & Martha B. Koo. 2016. Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research.
3) Balaji Anbil. 2018. "How we're investigating Digital Ledger Technologies to secure digital evidence" GOV.UK blogpost. 〈https://insidehmcts.blog.gov.uk/2018/08/23/how-were-investigating-digital-ledger-technologies-to-secure-digital-evidence/〉
4) Smart Dubai 〈https://smartdubai.ae/〉

한편 블록체인 기술 운영의 표준화된 지침 개발과 상호운용성 확보가 필요함에 따라 ISO TC 307 Blockchain and distributed ledger technologies[5]에서 블록체인 기술의 표준화 연구가 진행 중이며, 한국도 표준화 작업에 참여하고 있다.

국내의 블록체인 연구는 정보통신기술 분야의 연구가 주를 이루고 있다. 기술 구조 및 적용, 시스템 보안에 관한 연구가 많으며, 비즈니스 경영 분야의 연구가 진행되었다. 주목할 점은 공공기관을 중심으로 블록체인의 도입 가능성을 검토하는 사례가 늘고 있다는 것이다. 최근 행정안전부, 한국인터넷진흥원 등의 기관을 중심으로 블록체인 적용 분야를 적극적으로 탐색하며 시범사업을 추진하고 있다.

그러나 블록체인 기술에 관한 기록학 분야의 연구 성과는 매우 드물다. 2017년 국가기록원의 연구과제 "차세대 기록관리모델 재설계 연구"[6]는 블록체인과 관련하여 UBC프로젝트와 ISO 표준화 현황 등 국제 사례 등을 소개하며 블록체인 기술의 기록관리 적용가능성을 모색하는 논의를 시작하였다는 의의를 갖는다. 기록관리 분야도 새로운 기술의 적용가능성을 적극적으로 분석하고 활용분야를 다각도로 검토할 필요가 있다.

이러한 의미에서 이 연구는 블록체인의 기록관리 적용을 모색해보고자 하였다. 이를 위해 2장에서 블록체인의 주요 개념을 문헌 연구를 통해 살펴보고, 기록관리 적용가능성 탐색을 위해 기록관리 개념과 블록체인 개념의 접목지점에 대해 이 논문의 3장에서 중점적으로 다루었다. 4장에서 블록체인의 연구 성과 검토와 전자기록관리 프로세스를 고려하여 기록관리를 위한 블록체인 모형을 제안하였으며, 블록체인이 기록관리에 미치는 영향을 분석하여 정리하였다.

---

5) ISO/TC 307 "Blockchain and distributed ledger technologies" 〈https://www.iso.org/committee/6266604.html〉

6) 명지대학교 산학협력단 디지털아카이빙연구소. 2017.『차세대 기록관리 모델 재설계 연구 개발』. 대전 : 국가기록원.

2. 블록체인 기술의 이해

분산원장(distributed ledger) 기술로 대변되는 블록체인 기술은 그 자체로 진본인증 방안으로 활용될 수 있도록 블록 구조와 네트워크가 설계되었다. 개념적으로는 원본 기록을 불역적이고 불변경하게 영속적으로 유지할 수 있다고 할 수 있다. 전자기록의 진본인증과 관련하여 블록체인 기술의 개념을 검토하고자 한다.

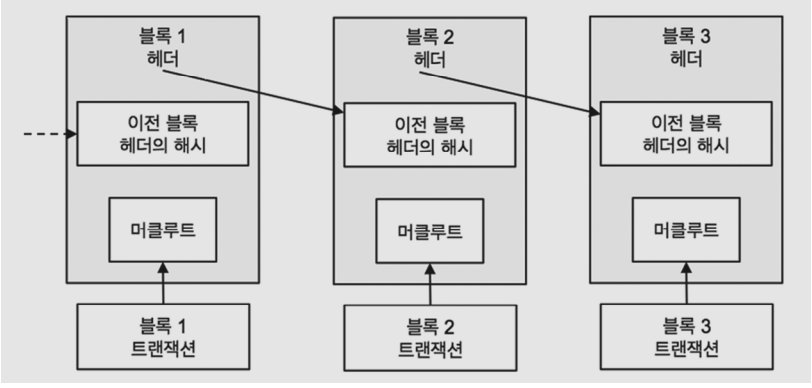
1) 블록체인의 구조

블록체인은 "공개적으로 접근가능하고, 분권화되고, 분산되며, 자동화된 원장에 저장된 거래기록을 신뢰할 수 있고 불변하도록 지원하는 오픈소스 기술"로(Victoria L. Lemieux 2017) 정의할 수 있다. 보다 구체적으로는 암호화한 거래 기록을 '블록' 단위로 시간 순으로 지속적으로 추가하여 유지하는 분산원장 기술이다. 여기에는 주목해야 할 개념이 담겨져 있는데, 암호화한 거래 기록을 탑재한 블록이 시간 순으로 연결되어 있다는 것과 분산원장이 갖는 의미를 잘 살펴보아야 한다.

분산원장은 동일한 원장 데이터를 네트워크에 참여한 모든 시스템이 보유하여 항상 동기화하고 상태를 공유하는 것을 뜻한다. 또한 거래 기록을 시간 순으로 이어서 앞 블록과 뒤의 블록을 연결하여 네트워크 참여자가 모두 저장하도록 하면 과거 블록 내용을 변경하기 위해서는 모든 참여자의 블록 내용을 변경해야 하는데 이는 사실상 불가능하므로, 거래 기록을 고정 불변하게 저장할 수 있는 것이다. 이러한 특성으로 위변조의 어려움, 거래의 유효성 검증의 효과를 갖는다.

블록체인의 구조는 다음 〈그림 1〉과 같이 블록 헤더와 트랜잭션을 기록한 블록 바디로 구분할 수 있다.

〈그림 1〉 간략화한 블록체인 개념



※출처 : Victorial L. Lemieux. 2016c, p.120.

블록의 정보를 담고 있는 블록 헤더의 값을 해시하여 다음 블록 헤더로 연결하고, 각 블록의 트랜잭션 데이터인 페이로드는 머클트리(Merkel Tree, Hash Tree)[7] 방법으로 해시하여 블록 헤더에 포함시킨다. 즉 하나의 블록 내에서 블록 내용을 해시하여 블록헤더에 넣음으로써 블록과 블록 헤더를 연결하고, 앞 블록의 헤더값을 해시하여 뒷 블록의 헤더에 넣어 앞 블록과 연결한다. 이러한 구조를 취함으로써 앞 블록 전체 내용을 해시하지 않고 블록 헤더만 해시하더라도 앞 블록 전체 내용을 해시하는 것과 같은 기능을 하게 되며, 보다 간단한 계산으로 체인에 연결할 수 있는 효과를 얻을 수 있다. 또한 블록을 연결하기 위해서는 앞선 블록의 해시를 확인하여 이상 없음을 증명한 후 체인으로 연결하게 되므로, 앞선 블록의 수정이나 삭제를 위해서는 이후 모든 블록을 수정해야 하므로 사실상 블록 내용의 수정이나 삭제가 불가능한 구조이다. 이러한 의미에서 블록체인의

7) Merkle Tree는 암호학 및 컴퓨터공학에서 해시트리 혹은 머클트리로 불린다. 데이터인 잎 노드(leaf node)에서 데이터 블록의 해시를 형성하고, 상위 노드의 해시값은 다시 해시함수로 계산하여 자식 노드들의 해시값을 구성한다. 머클트리는 대용량 데이터의 내용을 효과적이고 안전하게 검증하는 방법으로 활용된다(wikipedia "Merkle Tree").

길이가 길어질수록, 즉 블록이 누적될수록 그 무결성 보장은 강화된다고 할 수 있다.

블록 본문의 데이터인 페이로드를 어떻게 설계할 것인가는 블록체인 응용분야에 따라 다르게 구성할 수 있다. 해시 정보만 탑재할 것인지, 메타데이터를 함께 탑재할 것인지 다양한 모형으로 설계가 가능한데, 이는 기록의 특성과 진본확인을 위한 정체성, 무결성 입증 등의 목적에 따라 결정해야 할 것이다.

2) 주요 개념

블록체인의 핵심 기술이라 할 수 있는 해시함수, 합의 알고리즘, 분기의 해소 방법 등에 대한 이해를 바탕으로 기록관리 분야의 활용가능성을 검토할 수 있을 것이다.

(1) 해시함수

블록체인은 앞서 설명한 바와 같이 블록 헤더와 블록으로 구성되는데 블록 헤더에 이전 블록 헤더의 해시값과 블록 본문의 페이로드 해시값이 포함되도록 설계되었다. 해시는 디지털 데이터에서 해시함수를 통해 고유한 값으로 생성되는 것으로, 해시를 생성하는 해시함수는 디지털 데이터의 크기와 상관없이 고정된 크기의 해시를 생성한다. 어떤 길이의 디지털 데이터를 넣어도 해시함수를 사용하여 정해진 길이의 해시값을 생성하는 것이다. 암호화 해시 기술은 SHA-1, SHA-2, SHA-3 표준이 있다. SHA-1이 같은 해시값을 갖는 서로 다른 데이터 쌍을 찾는 충돌쌍공격에 성공하게 되며 SHA-2로 암호 마이그레이션이 되고 있다(김한기, 김종성 2019, 10). SHA-2 해시 군(family)은 224, 256, 384, 512 비트로 된 다양한 길이의 해시값이 포함되지만 SHA-1과 동일한 수학적 기반을 두고 있다. SHA-3은 SHA-1과

SHA-2와는 다른 구조로 설계되어 이전 버전의 결함을 보완하였으나 이를 지원하는 하드웨어의 복잡도 및 소프트웨어의 성능 평가 등이 연구되고 있는 단계이다.

해시함수의 핵심은 결과값의 충돌이 없도록 하는 것이다. 디지털 데이터가 단 1비트라도 변경되면 완전히 다른 해시값을 생성하므로 해시 비교를 통해 위변조 확인이 가능하다. 또한 데이터로부터 해시를 생성할 수 있지만 해시로부터 데이터를 표시할 수 없는 단방향 프로세스로서 보안성을 갖는다. 이러한 특성으로 전자기록이 변경되지 않았음을 증명하는데 활용할 수 있으며(Stephen Thompson 2017, 4-5), 생산된 당시의 해시값과 이벤트 과정 후 생성된 해시값이 다르므로 감사증적 및 사본 관리에도 활용할 수 있다.

하나의 블록 구성을 보면, 해당 블록의 페이로드 전체를 머클트리로 해시값을 구성하여 이전블록의 해시값과 연결하고, 임의의 난스(Nonce) 값을 첨부하여 블록을 구성한다. 블록 전체의 해시값에 임의의 난스값을 더하여 목표값과 비교하는 방법으로 유효한 난스값을 찾아 유효 블록을 생성해내는 것이다. 이 난스값을 찾아내는 연산작업의 처리 속도에 따라 목표값을 조정하기도 한다. 이렇게 생성된 블록을 네트워크에 전파하여 각 노드가 받아들여 체인으로 연결되는 것이다. 이러한 방법으로 블록을 생성하기 때문에 어느 한 블록의 내용을 변경하게 되면 다음 블록의 해시값이 변하게 되고 이후의 모든 블록 해시를 다시 계산해야 하므로 사실상 위조나 변조가 불가능하므로 전자기록의 인증에 활용할 수 있는 것이다.

⑵ 합의 알고리즘

P2P(Peer-to-Peer) 네트워크를 이용한 분산 원장 기술에서는 네트워크 참여자간의 정보 도달에 시간차가 존재하게 되는데, 하나의 결과에 대한 합의를 얻기 위한 방안이 필요하다. '비잔티움 장군 문제'로 불리는 상호 통신을

통한 합의 과정에서 악의적인 정보 변경 등의 문제 상황이 발생할 경우, 올바른 합의에 이르기 위한 합의 알고리즘이 요구된다. 블록체인은 분산된 모든 노드가 동일한 원장을 보유하기 위해 각 노드에서 생성된 블록의 정당성을 확인하고 공유하기 위한 합의 알고리즘을 사용한다(아카하네 요시하루 외 2017, 105). 합의 알고리즘에는 작업 증명(Proof of Work)과 지분 증명(Proof of Stake) 방식을 비롯하여 다양한 알고리즘이 있다.

가장 많은 블록체인 기반 기술이 채택하고 있는 알고리즘은 작업 증명 방식이다. 작업 증명 알고리즘은 네트워크 참여 노드들이 이전 블록 헤더의 해시값과 해당 블록 페이로드 해시값에 난스 값을 합한 값을 해시하여 특정 값을 찾아내는 연산 작업이 필요하다. 해시를 역연산하여 특정 값을 찾아내기 위해 난스를 변화시키며 순차적으로 대입하는 연산 과정을 거쳐야 하므로, 컴퓨팅 파워가 높은 노드일수록 블록 생성 시간이 단축된다.

작업 증명 알고리즘은 유효한 새로운 블록을 생성하는 마이닝(Mining)에 소모되는 전력량이 높아 에너지 효율이 떨어지고, 트랜잭션 내용을 검증하고 새로운 블록을 각 노드로 전파하고 체인에 추가하는 과정에 소요되는 시간이 길어 효율성이 떨어진다는 단점이 있다. 기록관리에 적용하기 위한 블록체인 모델에는 네트워크 참여 노드의 특성과 기록의 특성을 고려하여 합의 알고리즘을 설계할 필요가 있다.

⑶ 분기의 해소 방법

블록체인은 네트워크에 참여하는 개별 노드들이 자율적으로 블록을 생성하면서도 합의 과정을 통해 모든 노드가 동일한 원장을 갖도록 하는 것이 핵심이다. 그러나 새로운 블록을 생성하는 마이닝 과정에서 특정 시점에 하나 이상의 유효한 블록이 생성되는 경우가 발생할 수 있고, 이때 개별 노드들이 블록을 선택하는 것에 따라 체인이 다르게 구성될 수 있는데,

이를 '분기(fork)'라고 한다. 이를 해결하기 위한 방법으로 '긴 체인(Longest Chain) 선택 방식'이 있다.

서로 다른 노드에서 동시에 생성된 각각의 블록은 독자적으로 퍼져나갈 것이며, 앞선 블록의 해시값을 포함하여 다음 블록을 생성하게 되므로 각 블록은 별개의 체인을 형성하게 된다. 그러나 각 노드는 전파된 블록을 확인하고 체인에 연결하는 과정에서 독자적으로 퍼져나가는 체인 중 더 긴 체인을 받아 연결하고 다음 새로운 블록을 마이닝 하기 위해 경쟁하는 것이 유리하므로 짧은 체인을 버리고 긴 체인을 선택하게 된다. 결국 하나의 블록체인이 남게 되는 것이다. 누구나 참여 가능한 퍼블릭형 블록체인에서는 동일 원장을 유지하기 위해 유효한 방법이다. 그러나 기록관리를 위한 블록체인은 이러한 방식보다는 기록관리 기관으로 참여 기관이 제한된 네트워크에 적합한 합의 알고리즘을 개발하여 적용할 필요가 있다.

3. 진본인증을 위한 블록체인 기술 적용가능성

블록체인 기술의 기록관리 적용가능성 탐색을 위해 기록관리와 블록체인 개념의 접목지점에 대해 중점적으로 검토해보고자 한다. 블록체인은 블록에 탑재된 데이터를 변경 없이 영속적으로 유지하며, 그 출처 및 이력을 추적하기에 적합한 기술이므로 기록관리 분야에 적용한다면 기록의 진본성과 무결성을 보장할 수 있고, 이를 기반으로 신뢰할 수 있는 기록관리 체계를 구축할 수 있을 것이다.

3장에서는 블록체인의 기록관리 활용에 가장 핵심적인 부분이라 할 수 있는 진본 인증 방안으로서의 활용 가능성을 검토해보고자 한다. 이를 위해 기록의 진본성 개념의 이해를 바탕으로 새로운 블록체인 기술을 진본인증 방안으로 활용하기 위한 이론적 검토를 진행하였다.

1) 진본인증 개념

기록의 특성으로서 갖추어야 하는 품질요소로 ISO 15489에서는 진본성, 신뢰성, 무결성, 이용가능성을 들고 있다. 기록의 품질로서의 진본성(authenticity)은 기록이 기록으로서 갖는 신뢰가치, 즉 기록이 표방하는 바 그대로의 기록이면서 변조나 훼손되지 않은 상태로서 갖는 품질로 정의된다.[8)]

설문원의 연구에서는 서양의 기록학 문헌들에 나타는 진본성 개념을 범주화하였다. 진본성을 신뢰성, 무결성, 이용가능성을 포괄하는 개념으로 이해하는 광의의 진본성 개념과 무결성과 유사한 범주를 구성하는 협의의 진본성 개념으로 구분하였다. 광의의 진본성은 신뢰성, 무결성, 이용가능성을 충족해야 진본성을 '추론' 내지는 '추정'할 수 있다고 보았다(설문원 2005, 63-64). 반면, 협의의 진본성을 따르는 대표적인 연구 InterPARES에서는 진본성을 구성하는 요소로서 무결성과 정체성을 들고 있다. 또한 기록이 생산, 수신되고 저장되는 기록관리시스템의 무결성과 기록관리 프로세스의 신뢰성이 입증된다면 진본임을 선언할 수 있다고 보았다(Government of Canada 2017, 9). 즉 진본성은 시스템의 무결성과 기록관리 과정의 신뢰성으로 확보된다고 할 수 있다. 본 연구에서도 InterPARES의 진본성 개념에 대한 이해를 기반으로 한다.

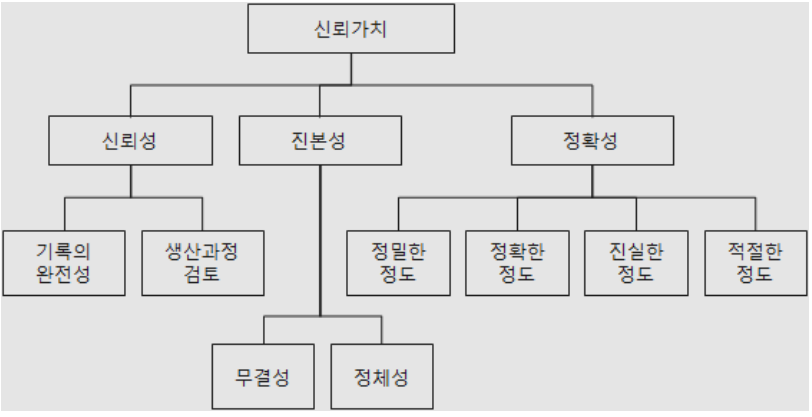
InterPARES에서는 다음 〈그림 2〉와 같이 기록 특성과 개념의 관계를 이해할 수 있도록 기록 개념에 관한 온톨로지를[9)] 정의하였다.

---

8) InterPARES 2 Project Dictionary. "authenticity" [version 2018. 1.] [http://www.interpares.org/ip2/display_file.cfm?doc=ip2_dictionary.pdf&CFID=14856066&CFTOKEN=48477459]

9) InterPARES 2 Project Ontology C : Trustworthiness of a Records [http://www.interpares.org/ip2/display_file.cfm?doc=ip2_ontology.pdf]

〈그림 2〉 기록의 신뢰가치 온톨로지



※출처 : InterPARES 2 Ontology. 2008, p.3.

이 온톨로지에 따르면 기록의 신뢰가치는 신뢰성, 진본성, 정확성의 정도에 의해 부여된다. 신뢰성은 완전성과 생산과정에 의한 검토로 확인되며, 정확성은 엄밀함, 정확함, 진실함, 적절함의 정도를 의미한다. 진본성은 무결성과 정체성으로 구성되는 개념으로서, 정체성은 기록을 고유하게 확인하여 다른 문서나 기록으로부터 구분할 수 있도록 하는 특성을 의미한다. 정체성은 저자, 수취인, 작자, 원작자, 날짜, 행위, 이벤트 명칭, 전송상태, 다른 기록과의 관계로 구성되며, 무결성은 총체성(wholeness)과 견실성(soundness)으로 구성된다. 진본성은 기록의 정체성을 확인하고 무결성을 증명함으로써 성립한다고 할 수 있다.

신뢰성이 기록 생산에 관련된 개념인 반면, 진본성은 전송 및 보관 상태에 관한 개념이다. 신뢰성은 기록된 사실에 대한 진술의 신뢰가능성을 측정하는데 반해, 진본성은 기록이 생산된 당시의 본래 실체와 그 기록이 지속적으로 유지되었는지에 관한 평가인 것이다. 기록이 진본임을 선언하는 것은 기록을 보존하기 위해 따로 옮겨지거나 이동될 때의 그 당시와 정확

하게 동일함을 입증하는 것을 의미한다(Luciana Duranti 2017, 454). 또한 기록 보존의 투명성, 보안성, 안정성의 필수 요인에 의해 진본성이 확보된다(Luciana Duranti 2017, 460). 즉 생산과정의 무결성 증명을 통해 신뢰성을 확보하고, 보존 과정의 무결성 증명을 통해 진본성을 확보할 수 있는 것이다.

Lemieux는 진본성을 구성하는 정체성이 기록의 결합관계와 관련이 있다고 정의하였다. 기록은 "활동의 도구나 부산물로서 활동 과정에서 만들어지거나 수신된, 활동이나 참고를 위해 따로 두어진" "지적 객체"로서 "어떤 기록은 그것이 기록된 활동과 그것을 기록으로 유지한 주체와 동일 활동내의 다른 기록과 명확한 관계를 갖는데(ISAAR(CPF))", 이 관계가 기록의 결합관계를 의미한다. 이는 특정 생산 및 이용 맥락과 연결하는 것뿐만 아니라 기록이 속한 특정 기록 집합의 관계도 정의하기 때문에 진본성 판단에 필수적이다. 정체성과 함께 진본성을 구성하는 무결성에는 접근 통제, 사용자 인증 및 검증, 감사 추적, 시스템의 정상적 기능 운영 입증, 정기적 유지보수 및 업그레이드 빈도에 관한 문서화 등의 시스템 무결성 입증이 포함된다(Victoria L. Lemieux 2017, 4).

진본 기록의 사전적 의미는 그것이 의미하는 바 그대로 변조되거나 훼손되지 않은 기록[10]을 의미한다. 진본기록임을 확인하는 요건으로 ISO15489에서는 그것이 생산된 취지와 일치하여 존재하는지, 그것을 생산하거나 보낸 것으로 되어 있는 그 사람에 의해 생산되거나 보내졌는지, 명시되어 있는 시간에 생산되거나 보내졌는지 증명되어야 함을 들고 있다(ISO15489-1 : 2016, 5.2.2.1).

전자기록관리 환경에서 기록의 진본성의 논의가 더욱 중요한 이유는 전자기록의 구조적 차이에서 발생한다. 종이기록이 물리적 요소인 컨테이너와 지적 요소인 내용이 결합되어 있는 반면, 전자기록은 내용정보와

10) InterPARES 2 Project Dictionary, version 2018.01. "authentic record"

모든 구성 요소들이 분리되고, 컨테이너의 구성 요소들은 지속적으로 변화하며 재생산되기 때문이다(김익한 2006, 95-96). 전자기록의 이러한 특성상 위변조의 위험성이 존재하므로 진본 기록임을 증명하는 것은 중요한 문제이다. 전자기록의 재현을 위한 기술 의존성 증가에 따른 문제 및 끊임없는 재생산 과정에서 재생산 전과 후의 진본 확인 과정에 대한 연구가 필요하다.

2) 진본인증을 위한 블록체인 기술 활용

블록체인을 기록관리에 적용할 경우 현재의 진본인증 체계에 어떤 변화를 줄지 전망해 볼 필요가 있다.

블록체인은 한번 블록에 저장한 기록은 변경할 수 없는 특성을 갖고 있다. 이것은 기록의 감사증적 및 증명에 매우 유용한 개념이 될 것이다. 더 나아가 이것은 기록이 생산된 바 그대로 유지되었다는 기록의 진본성과 위변조나 손실되지 않고 유지되었음을 나타내는 무결성의 기록 가치를 입증하는데 활용될 수 있다. 또한 기관 간의 기록의 수신·발신, 이관, 기록관리 활동의 처리 결과를 입증하고 증명하는 데에도 유용한 개념이다.

블록체인 네트워크 전체에 기록 변경 이력을 분산저장하면, 저장된 정보가 변경되지 않고 유지되는 특성으로 그 자체가 진본성을 입증하고 보장하는 방법이 된다. 진본 인증 요구가 발생할 때마다 분산되어 있는 정보를 꺼내어 확인하는 방법으로 진본 인증이 가능하다. 기록 컴포넌트와 메타데이터는 기존의 생산기관 및 기록관리기관의 저장장치에 두고 해시정보의 공유만으로도 진본인증이 가능하므로 인증정보를 통한 인증방식과 시점인증 방식에 기반한 현재 인증 체계에도 변화를 줄 수 있다. 뿐만 아니라 기록의 유통과 공유 체계에도 영향을 미칠 것이다.

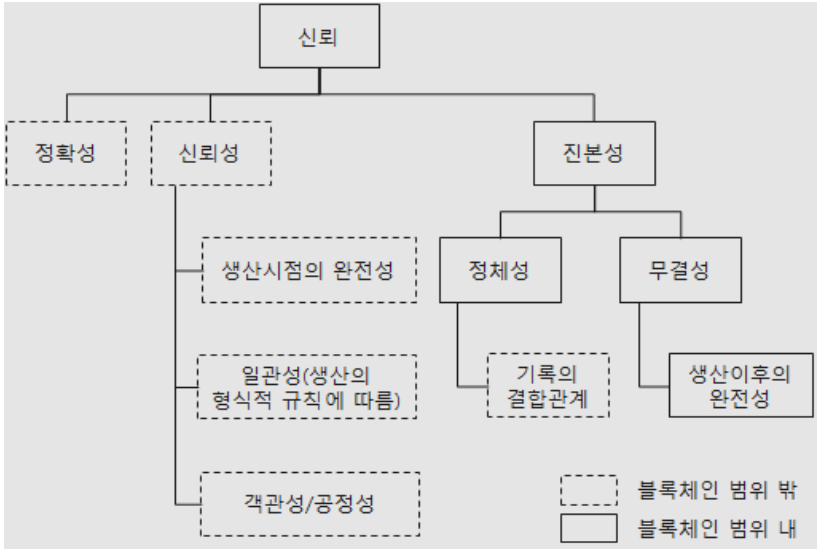
기록과 그 인증정보까지 중앙집중형으로 저장하던 기존의 방식에서는 그 관리주체의 권한과 부담이 커지게 되고 위험부담도 커질 수밖에 없다. 그러나 분산화된 체계에서는 기록관과 영구기록물관리기관과 같은 중앙집중형 권력 구조를 보이는 것이 아닌 네트워크에 참여하는 노드의 역할이 중요해진다. 패러다임의 변화가 가져올 기록관리 체계의 근본적 변화를 예측하고 준비해야 한다. 기존의 처리과 → 기록관 → 영구기록물관리기관 단계의 분절적인 기록관리 체계가 아닌 생산 이후 관리와 유지를 위한 조치가 함께 이루어지고 이 정보의 공유를 통한 기록이 무결성과 진본성, 신뢰성이 보장되는 프로세스가 마련되어야 한다.

기록관리에 블록체인이 적용된다면 기록이 생산된 이후 그 기록의 출처를 확인할 수 있고, 기록관리 과정의 이력과 무결성을 입증할 수 있다. 이를 통해 기록의 신뢰성을 확보하고 나아가 신뢰할 수 있는 기록관리의 기반 마련에 기여하는 효과를 얻을 수 있을 것이다.

그러나 현재의 블록체인 기술을 적용하기 위해서는 기록관리 측면의 고려사항이 상당부분 반영되어 개선되어야 한다. 실제 컨텐츠 대신 해시만 블록체인에 기록되는 시스템에서는 기록의 생산 과정 및 그 통제가 블록체인 시스템 운영 범위 내에 있지 않으므로 기록의 정확성과 신뢰성을 확보하기 어렵다. 또한 기술적 관점에서 블록체인 네트워크 노드간의 블록이 불일치하거나, 시스템의 구성요소의 오류나 불일치 등은 정확성에 영향을 미칠 수 있다.

블록체인 기술을 기록관리에 적용하기에 앞서 기록의 속성과 어떤 관계가 있으며, 어떤 속성을 지원하는지 분석할 필요가 있다. 블록체인 기술은 신뢰할 수 있는 기록을 구성하는 요건인 정확성과 신뢰성에는 영향을 미치지 않는다. 다만, 진본성을 보장하는 방안으로 활용할 수 있다. 이는 다음의 〈그림 3〉으로 표현된다.

〈그림 3〉 블록체인 기술의 기록관리 측면 평가



※출처 : Victoria L. Lemieux. 2017, p. 7.

정확성은 기록이 담고 있는 정보에 부여되는 가치이며, 신뢰성은 기록의 생산과정에 대한 검토로 판단되는 속성이므로 블록체인이 보장하는 정보의 무결한 유지나 증거적 기능과는 관련성이 없다. 진본성은 본래 생산된 의도대로 기록이 유지되었는가를 평가하는 가치이므로 블록체인의 개념을 적용하여 진본성 보장 방안으로 활용할 수 있다.

기록의 정체성과 관련하여서도 기록의 결합관계에 관한 블록체인 기능이 현재로서는 존재하지 않는다. 따라서 맥락정보를 담고 있는 메타데이터를 블록체인의 페이로드에 포함하는 방안을 고려해야 할 것이다. 무결성 보장은 블록체인 기술을 적용할 때의 이점으로 논의되고 있으나 시스템의 보안 위험이나 오류 등의 블록체인 시스템의 취약성에 대한 대책도 고려되어야 한다.

4. 기록관리를 위한 블록체인 모형 설계

블록체인 기술의 주요개념을 기록관리에 적용하여 기록의 진본성과 무결성 보장을 위한 개념모형을 제안하고자 한다. 블록체인 네트워크의 구성과 블록의 구조를 제시하고, 기록의 생산과 관리에 활용가능한 기록관리 블록체인 모형을 제안함으로써 디지털 환경 변화에 조응하는 신뢰할 수 있는 기록관리 체계를 모색해보고자 한다.

1) 기록관리를 위한 블록체인 개념 설계

(1) 네트워크 형태

전자기록은 생산된 이후, 지속적으로 재생산되며 관리되고 활용된다. 기록을 생산하고, 이관하고, 매체변경, 정보패키지의 변경 등의 이벤트가 발생할 때마다 전자기록의 특성상 재생산 과정을 추적하여 진본임을 인증할 필요가 있다. 이벤트의 전 과정이 기록되어 추적할 수 있어야 하며, 그 결과에 대해서도 진본임을 확인할 수 있어야 한다. 시스템 인프라 측면에서 진본 추정에 신뢰성을 더하는 방법으로 분산원장 기술을 적용하면 시스템이 자동화된 방식으로 진본 확인 작업을 수행하여 진본 추정력을 강화할 수 있을 것으로 판단한다.

물론 분산원장 기술이 기록의 신뢰성과 무결성을 증명하는 것은 아니다. 단지 기록의 관리과정에서 유지 및 보존, 활용의 조치가 취해진 시점 이후 인가받지 못한 변경이 있었는지의 여부를 확인하는 데 활용할 수 있다.

블록체인 기반 기술은 용도와 적용되는 네트워크 종류에 따라 구분할 수 있는데, 누구나 참여 가능한 퍼블릭(Public)과 신뢰하는 참가자로만 제한하는 컨소시엄(Consortium) 및 프라이빗(Private)으로 나눌 수 있다. 퍼블릭은 노드의 제한이 없고 블록의 검색에도 제한이 없다. 그러나 기업 및 기관 간

에 신뢰하는 참가자로만 구성하는 컨소시엄형이나 단일 조직 내에서 운영하는 프라이빗 블록체인 형태는 노드를 제한하고 블록체인의 검색도 제한된다(아카하네 요시하루 외 2017, 90-91).

누구나 참여할 수 있도록 개방되어 있는 퍼블릭형 블록체인은 블록에 저장되어 있는 트랜잭션의 내용을 참여자 모두 공유하기 때문에 개인정보보호 및 보안의 문제가 발생할 우려가 있다. 또한 새로운 블록을 생성하는데 시간과 비용이 소요되고 모든 노드로 블록을 전파하고 승인하는 데에도 시간이 길어진다는 단점이 있다.

따라서 기록관리 분산원장의 아키텍쳐를 제안하는데 있어 전제되어야 할 조건은 사전에 협의된 아카이브 기관만 인증 받아 네트워크를 구성하는 노드로 참여할 수 있도록 제한하는 것이다. 기록의 생산과 관리는 접근권한과 공개여부에 따른 보안이 요구되는 분야이므로 사전에 허가받은 참여자들만 네트워크를 구성하게 하고, 새로운 블록 형성을 위한 마이닝 작업과 전체 노드로 블록을 전송하고 승인받는 절차를 합의 과정으로 간소화하여 속도와 비용면에서도 효율적으로 운영할 수 있다. 이러한 측면에서 기록관리에 적용가능한 블록체인 네트워크 모형은 컨소시엄형으로 구분할 수 있다. 기록관리 블록체인 노드에 참여하는 기록관리 기관은 노드간의 합의 형성 알고리즘을 생성하여, 분산원장을 공유할 수 있는 체계를 구축해야 한다. 여기에서의 분산원장은 기록관리시스템 및 아카이브 시스템과는 분리된 별도의 네트워크 체계를 구성하는 것으로 이러한 조건이 전제되어야 한다.

네트워크에 참여하는 분산 노드에는 기록관리 기관만이 아니라, 사회적 신뢰 기관의 역할을 할 수 있는 관련 학회나 협회, 대학기관과 같은 기관도 참여시켜서 블록체인 분산원장의 공공의 신뢰를 높이는데 기여할 수 있다. 아카이브 기관에서 생산되어 관리되고 보존된 기록의 진본성과 무결성 입증 방안으로서 블록체인의 활용은 개별 기록의 진본인증 수단을 넘어서 기록관리의 공공의 신뢰 체계를 구축하는 의미를 갖는다. 따라서 참여 노드의 아카이브 신뢰성 제고 전략으로 활용될 수 있을 것이다.

⑵ 블록의 구성

전자기록에 적용할 수 있는 블록체인의 블록을 구성하는데 있어 가장 중요한 핵심은 전자기록의 진본 입증을 지원하는 기능을 구현하는 것이다. 전자기록이 생산된 이후 모든 기록관리 행위에 대한 감사증적이 가능해야 하며, 이를 통해 무결성이 보장되어야 한다. 앞서 검토하였듯이 무결성이 충족되어야 진본 인증이 가능하다. 이 과정은 기록관리의 신뢰성을 확보하기 위한 것이기도 하다.

기록관리에 적용할 수 있는 블록체인 실행을 위해 기록 컴포넌트 자체를 블록체인에 탑재하는 모형을 생각해 볼 수 있다. 기록을 블록체인에 직접 저장하였기 때문에 개념적으로 블록에 탑재된 기록은 생산된 디지털 질서 그대로 불변하게 보존할 수 있다.

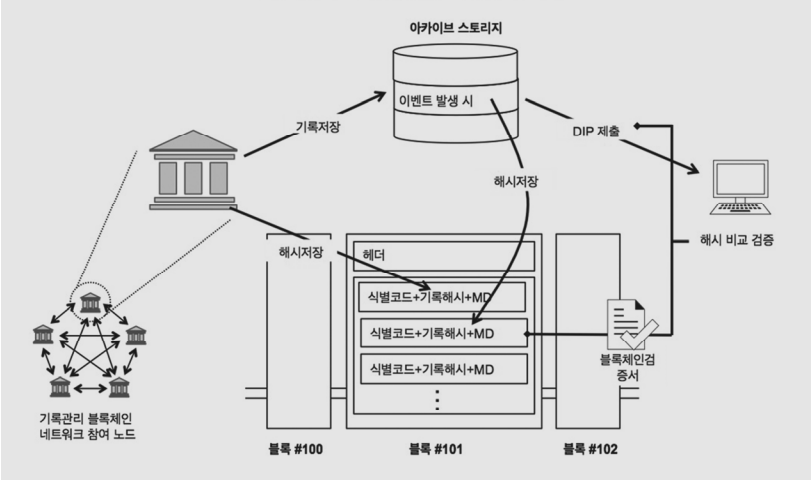
하지만 기록 컴포넌트 자체가 블록을 구성하여 저장될 때는 몇 가지 한계와 고려사항이 있다. 기록 자체가 네트워크를 구성하는 피어에 분산 저장되므로 그 용량이 매우 커진다는 한계가 있다. 식별자와 기록을 구성하는 본문과 첨부파일 등의 컴포넌트와 메타데이터를 블록의 페이로드에 탑재한다면 블록 하나의 용량은 매우 커질 것이다. 점차 다양한 유형의 매체에 기록되는 데이터가 많아지는데 이 모든 데이터를 블록체인 네트워크로 공유하는 것은 불가능하다. 또한 기록이 기관을 벗어나 다른 기관과 공유되기 때문에 개인정보보호와 비밀기록의 경우 제한을 받게 된다. 접근 권한 관리의 문제가 발생하는데 이에 대한 설정도 어렵게 된다. 따라서 이러한 모델의 경우에는 대상 기록을 한정하고, 매우 제한적으로 이용되어야 할 것이다.

따라서 기록관리 블록체인의 모형으로 〈그림 4〉와 같이 기록 정보 블록 생성 모델을 제안한다. 기관 내 또는 기관 간 기록관리 및 아카이브 시스템과는 별도로 분산원장 시스템을 P2P 네트워크를 구축한다. 분산 노드로 참여하는 기관에서 기록의 생산 시점부터 SIP(Submission Information Package)생성, AIP(Archival Information Package)생성, 기록관리 관련 메타데이터 정보

생성, 매체변환 시점, 사본 생성 시점, DIP(Dissemination Information Package) 생성 및 제공 등의 모든 이벤트가 발생할 때마다 기록을 관리하는 시스템은 동일한 해시 함수를 사용하여 해시를 생성하여 공유한다.

노드의 각 블록은 블록헤더, 기록관리의 데이터가 포함되는 페이로드로 구성된다. 블록헤더에는 앞 블록의 해시와 페이로드 해시가 포함된다. 블록에는 기록의 식별정보와 함께 기록의 생산 시점부터 기록관리 과정의 각 단계별로 기록의 해시가 생성되어 저장되며, 이에 대한 맥락정보도 함께 저장된다. 이벤트가 발생하여 해시를 생성하게 되면, 해시 생성시점과 컴포넌트의 식별정보가 해시와 함께 탑재되고, 기록관리 이벤트의 내용과 처리 결과, 다른 기록과의 관계에 대한 정보 등의 맥락정보를 담은 메타데이터가 함께 기재된다. 이렇게 형성된 하나의 블록은 각 기관 노드로 전파되어 체인에 연결된다. 이때 블록은 참여 기관 간 합의에 따라 일정시간마다 생성되도록 한다.

〈그림 4〉 기록 정보 블록 설계



이 모형에 따라 이벤트 이력 정보 저장 체인이 형성되어 공유된다고 할 수 있다. 기록을 구성하는 컴포넌트의 변경 상태가 가장 최신의 상태 정보로 업데이트 되어 저장되는 것을 의미하는 것으로서 감사증적으로 활용할 수 있으며, 진본 입증 방안으로 활용할 수 있다. 네트워크에 공유된 기록관리 분산원장은 기록의 진본인증 요청이 발생하면 블록체인에 탑재된 해시와 인증 대상 기록의 해시를 비교하여 진본임을 확인하는데 이용된다. 블록에 저장된 해당 컴포넌트의 최종 해시를 검증하여, "블록체인 검증서(Blockchain Verification Receipt)"를 자동으로 발행하도록 한다. 이 블록체인 검증서는 제출된 기록 해시와 블록체인 검증서의 해시를 비교 검증할 수 있도록 하는 것이다.

블록체인 검증서는 거래처리시스템(Transaction Processing System)[11]의 방식으로 발행된다. 기록의 진본인증이 필요한 시점에 블록체인 검증 요청이 발생되면, 데이터의 자동 검증 장치를 통해 시스템에서 자동적으로 블록체인에 저장된 데이터 중에서 해당 기록의 식별정보를 검색하여 해시를 확인하고 검증서(receipt)를 발행한다.

네트워크에서 분산 원장을 공유할 경우, 기관 내에서 진본 인증을 발급할 경우에 비해서 무결성 및 진본성 보장을 향상시킬 수 있다. 앞 블록을 증명하여 새로운 블록을 생성하게 되므로 블록체인이 길어질수록 신뢰도는 향상되기 때문이다. 한 기관 내에서 소장 기록의 진본 인증을 발급하게 될 경우 위변조의 위험성을 배제할 수 없다. 의도적 수정의 가능성을 볼 때, 여러 기관이 분산 저장할 경우보다 상대적으로 용이하기 때문이다.

또한 정보의 중앙집중형 관리체계에서는 중앙 시스템의 해킹과 같은 보안 위험성에 더욱 취약하다. 그러므로 다수의 참여 노드에 공유하고 분산

11) 거래처리시스템(Transaction Processing System)은 자재 구입, 상품 판매, 영수증 발행, 급여 지급, 온라인 입 · 출금, 신용도 관리, 상품의 주문 · 발송 등 거래와 관련된 데이터가 발생할 때마다 단말기에서 발신된 데이터를 수신 · 처리하여 그 결과를 즉시 보내주는 시스템이다(wikipedia "거래처리시스템").

저장하는 이점은 신뢰성의 확보와 감사증적의 특성에 있다.

또 다른 측면에서 분산 저장의 장점은 기관간의 유효성 검증에 대한 공통기준이 없는 경우 각 기관별로 유효성 검증 방안이 달라 검증이 어렵다는 것에 있다. 따라서 분산 노드에 저장되어 있는 블록체인을 확인하여 검증하는데 활용할 수 있다.

(3) 합의 알고리즘

기록관리를 위한 블록체인은 사전에 협의된 기관 간의 컨소시엄 형태로 네트워크를 구성한다. 컨소시엄형 블록체인에 많이 쓰이는 합의 알고리즘은 PBFT(Practical Byzantine Fault Tolerance) 프로토콜이다. 작업 증명 방식과 지분 증명 방식의 단점인 파이널리티 불확실성(finality uncertainty)[12]과 성능문제를 해결한 방법으로 신뢰할 수 있는 노드만이 참가하도록 허가되는 블록체인에서 블록을 생성하는 방법이다.

PBFT는 악의적 노드가 참가하는 경우인 비잔틴 장군 문제를 해결하고 블록체인이 동작하도록 하는 프로토콜이다. 네트워크 참여 노드 중 하나를 리더 역할을 하는 주요 노드(primary node)로 정하고 주요 노드가 주도하여 요청을 처리하고 관리한다. 클라이언트의 요청을 주요 노드가 각 노드로 명령을 전달하고, 명령이 수신된 각 노드는 모든 노드로 회신한다. 회신을 받은 각 노드는 모든 노드에 수신한 신호를 전송하고, 명령을 실행하고 블록을 등록하여 결과를 전송한다.

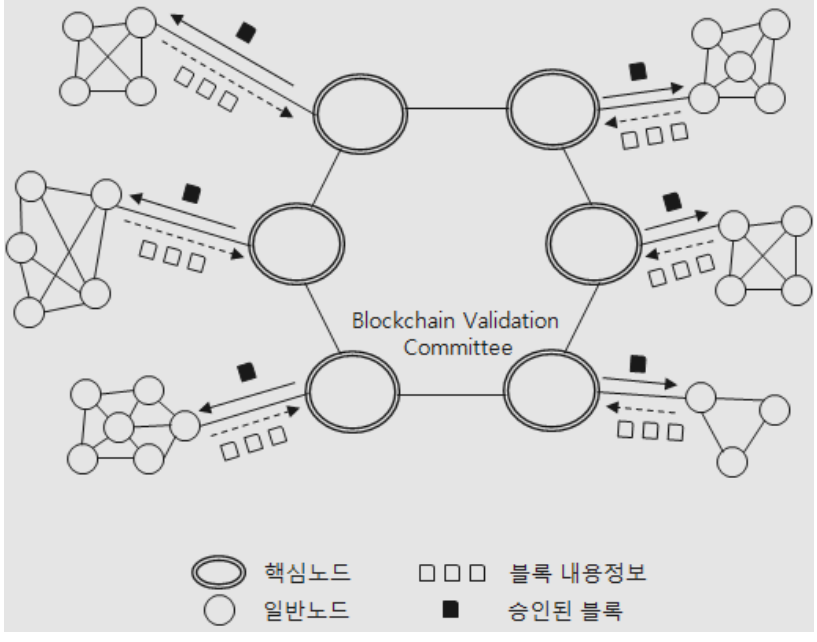
이러한 형태의 블록체인은 검증자 역할을 하는 특정 노드를 더욱 신뢰할 수 있다는 전제를 하기 때문에 기존의 중앙집중형 시스템과 마찬가지로 특정 관리주체의 신뢰성에 의존하게 된다는 비판을 받기도 한다(남충현 2018,

12) 블록체인이 분기하는 경우 짧은 체인을 사용하고 있던 노드가 긴 체인의 블록으로 전환할 때 짧은 체인의 트랜잭션이 긴 체인으로 수렴되어 모두 반영되기까지 시간이 소요된다. 따라서 결제완전성(finality)이 불확실하다는 단점이 지적된다.

9-10). 그러나 허가형 블록체인도 여전히 분산원장이 주는 이점을 유지하고 있으며, "블록체이닝(blockchaining)하는데 단 한가지의 옳은 방법이 있다는 생각은 완전히 잘못된 것"[13]이라는 의견이 합리적이라 판단된다. 그러므로 기록관리의 특성을 반영하여 책임성과 신뢰성 있는 기록관리 블록체인을 허가형으로 설계하여 사용할 수 있을 것이다.

PBFT의 주요 개념을 기록관리를 위한 블록체인에 적용하여 〈그림 5〉와 같은 합의 알고리즘 모형을 제안하였다.

〈그림 5〉 기록관리를 위한 블록체인의 합의 알고리즘



기록관리 블록체인 네트워크에 참여하는 노드는 핵심 노드와 일반 노드

13) Vitalik Buterin. 2015. On Public and Private Blockchains. Ethereum Blog [2015-08-07]

로 구분한다. 블록을 생성할 수 있는 권한을 가진 핵심 노드(Key node)는 단일한 primary 노드가 아니라 합의에 의해 여러 개의 노드를 지정할 수 있다. 핵심 노드들은 합의 기관인 블록 검증 위원회(Blcokchain Validation Committee)를 구성한다. 블록 검증 위원회에서는 생성된 블록의 유효성을 심의하고 합의에 의해 블록으로 생성하는 역할을 담당한다.

블록의 생성 과정은 다음과 같다. 핵심 노드는 일반 노드에서 수신되는 블록의 내용정보, 즉 페이로드 데이터를 종합하여 블록을 생성한다. 생성된 블록은 핵심 노드들의 합의 과정을 거쳐 블록 검증 위원회 승인을 받아 유효 블록으로 승인되어 모든 노드로 전파된다.

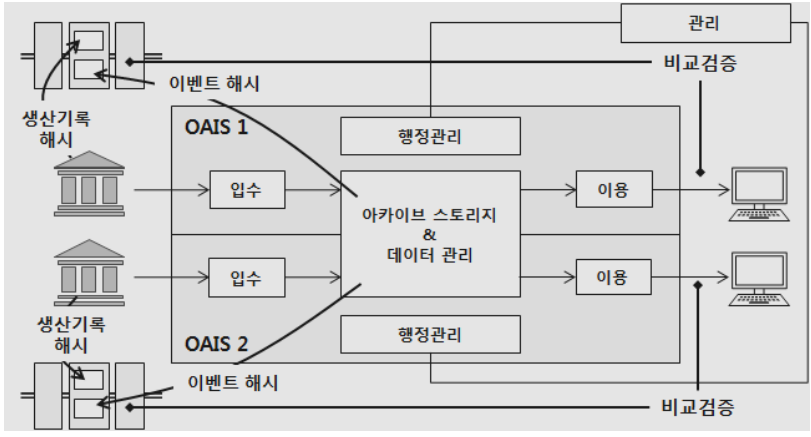
여기에서 합의 알고리즘에 신뢰성 강화를 위한 몇 가지 개념을 추가할 수 있다. 블록을 생성하는 핵심 노드에서 발행한 블록이 블록 검증 위원회의 검증을 받아 유효 블록으로 승인되고 전파되는 과정에서 핵심 노드들의 전자서명을 추가할 수 있다. 다중 서명 기술을 적용하여 핵심 노드들의 복수의 키로 서명하여 블록을 발행하게 되면, 블록의 조작 위험으로부터 보안성을 강화할 수 있다. 다중 서명에 필요한 모든 키를 획득해야만 블록의 생성이나 수정이 가능하기 때문이다.

한편 블록체인의 채널을 다중화하여 설계할 수 있다. 보안이 더욱 요구되는 기록의 정보나 인증 정보 등은 사이드 체인을 설계하여 따로 보관하는 방법을 강구해볼 수 있을 것이다.

2) 기록관리를 위한 블록체인 모형 제안

블록체인 모형 설계의 목적은 기록관리 활동 과정에서 위변조의 위험으로부터 기록을 보호하고 보존된 기록을 신뢰할 수 있도록 하는 과정을 지원하는 것이다. 전자기록관리에 적용가능한 블록체인 모형을 다음 〈그림 6〉과 같이 제안한다.

〈그림 6〉 클라우드 환경에서의 블록체인 모형



제안한 모형에 사용된 아카이브의 OAIS 참조모형에서 제안한 아카이브 상호운용성 모델 가운데 스토리지를 공유하는 아카이브 모델(CCSDS 2012, 6-8)이다. 모형에서 두 기관은 아카이브 스토리지를 공유하는데 이 공유된 스토리지는 클라우드 형태이든, 클라우드 형태가 아니든 제한을 두지 않는다. 이 두 기관은 저장과 데이터 관리 기능을 공유하지만 독립적으로 서비스를 제공할 수 있다. 그러나 입수-저장 및 접근-저장 간의 인터페이스 표준은 마련되어야 한다.

아카이벌 스토리지와 데이터 관리를 공유하는 이 장치가 클라우드 형태라고 가정한다면, 그림과 같이 블록체인과 아카이브간의 관계가 형성된다. 기록의 해시는 단계별로 생산되는데 먼저, 생산자가 기록을 생산하면 동시에 기록의 해시(생산기록 해시)가 생성되어 해당 기록의 메타데이터와 함께 블록에 저장된다. 그리고 생산된 기록이 아카이브 스토리지로 저장되어 기록관리 활동 과정 중 변경이 생길 때마다 이벤트 해시(Events Hash)가 기록 변경과 동시에 생성되어 이벤트 메타데이터와 함께 블록에 저장되게 된다. 이용자에게 서비스 될 때, 블록체인에 분산 저장된 해시를 검증하고 블

록체인 검증서를 발행하는데, 블록체인에 저장된 해시값과 서비스 되는 기록의 해시값을 비교 검증하여 진본임을 인증하게 된다. 즉, 생산기록 해시와 메타데이터, 그리고 기록관리 과정의 이벤트 시점의 해시와 관련 메타데이터가 블록에 저장되는 개념이다.

이 과정을 OAIS 아카이브 기능 엔티티 구성도(CCSDS 2012, A-2)에 따라 기록관리 기능별 프로세스에서 해시가 발생되는 시점을 확인하면 다음과 같다.

입수 단계에서는 기록이 아카이브로 SIP 형태로 입수되는 시점, SIP를 AIP로 변환하여 저장하는 시점, AIP로부터 기술정보를 추출하거나 데이터베이스, 스토리지로부터 기술정보를 수집하여 메타데이터를 생성하는 시점에 해시 값을 생성하여 저장해야 한다.

디지털 객체 저장 단계에서는 AIP를 저장하고 저장식별정보를 통지하는 시점과 저장 포맷 변환 기능을 수행하며 생산 당시의 디지털 질서가 변경될 여지가 가장 큰 시점이 포함된다. 포맷 변환이라는 전자기록의 재생산 시점에서 정보 손실을 최소화하는 방안이 마련되어야 한다. 그리고 재난복구 기능에 따른 사본 생성 시점에서도 해시 정보가 저장되어야 한다.

이용 단계에서는 이용자 요청에 따라 객체의 DIP를 생성하는 시점과 DIP가 제출되는 시점에서 해시가 자동으로 생성되어 저장되는 매커니즘이 작동되어야 한다.

기록관리 기능 프로세스 상의 해시 생성 시점을 확인하고 해시 정보가 저장되어야 하는 지점과 저장 되어야 하는 정보를 구체화하는 연구가 이어져야 할 것이다.

3) 기록관리 거버넌스 기대효과

기록관리 거버넌스는 정보 거버넌스의 측면에서 정보의 평가, 생산, 저장, 이용, 보존 및 처분에 있어 바람직하고 설명책임성 있는 의사결정을 위

한 프레임워크로서, 조직이 목표를 달성할 수 있도록 정보를 효과적이고 효율적으로 사용하도록 하는 프로세스, 역할, 표준, 지표가 포함되는 개념이다(The Electronic Discovery Reference Model(EDRM) LLC 2011, 2). 기록관리 관련 주체들 간의 협력체계 구축은 정보 거버넌스의 토대를 이루며, 정보 거버넌스는 궁극적으로 민주주의 실현의 기반이 된다.

기록관리 기관 간의 협력 관계는 기존의 처리과 → 기록관 → 영구기록물관리기관의 3단계 분절적 관리단계에 따른 계층구조에서 벗어나 기록관리 거버넌스 측면에서 수평적 협력 관계를 지향해야 한다. 이러한 수평적 협력 체계 구현을 위해 블록체인의 분산원장 기술은 적합한 기술이다. 동일한 데이터가 각 노드에 동등하게 저장되고 데이터의 신뢰성을 서로 검증해주는 구조는 수평적 협력 체계 마련에 유용한 개념이다.

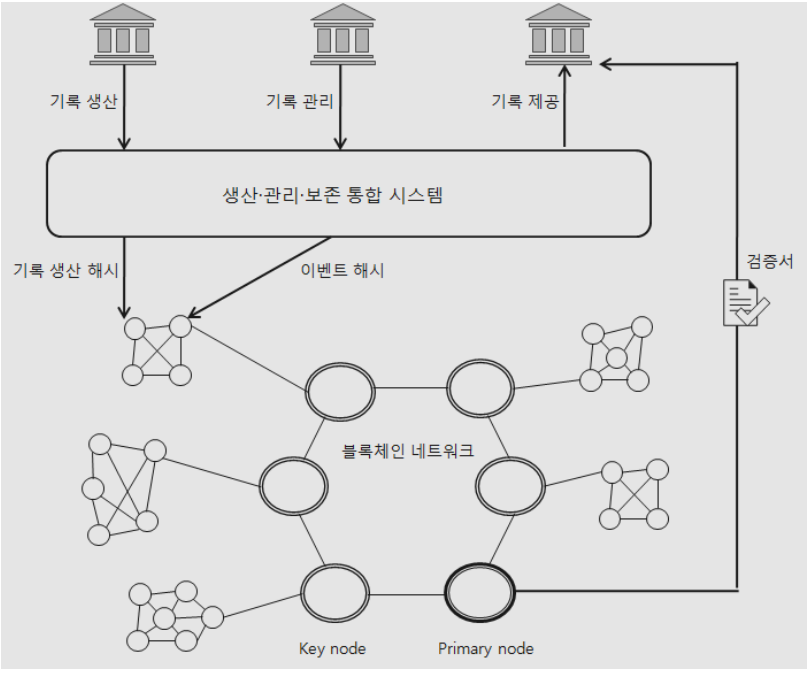
또한 수평적 협력 체계는 신뢰기반의 네트워크 구축이 전제되어야 한다. 데이터를 공유하고 유통하기 위해서는 기록관리 기관 간의 상호 신뢰를 바탕으로 네트워크가 구성되어야 한다. 블록체인 기술의 합의 알고리즘은 네트워크 기관 간 유통되는 데이터의 신뢰성을 보장하기 위해 설계되며, 각 노드를 구성하는 기관 간의 신뢰체계를 보장한다.

블록체인 모형의 적용가능성을 고려하여 제안한 기록관리 체계를 다음 〈그림 7〉과 같이 제안해 보았다.

이 모형은 블록체인 네트워크를 구성하는 기관 간의 역할을 도시하고, 기록을 생산하고 유통, 관리, 보존, 서비스하는 통합 시스템 체계를 나타내고 있다. 분권화된 기록관리 체계의 인프라에서 중요한 전제는 기록을 생산하고 관리하는 기관은 P2P 블록체인 네트워크로 연결되어 있고, 기관은 통합아카이브시스템에서 기록의 생산부터 보존 및 서비스 제공에 이르기까지 모든 기록관리 활동을 처리할 수 있다는 전제를 토대로 한다.

생산 · 관리 · 보존 통합 시스템은 기록의 생산과 관리 활동, 장기보존을 위한 아카이브 체계까지 갖추고 서비스하는 시스템으로 생산부터 장기보존에 이르는 기능을 포함한다. 기존의 기록관 및 영구기록물관리기관으로의

〈그림 7〉 분권화된 기록관리 체계 모형



물리적 이관이 아닌 논리적 이관으로 객체 정보과 관리 권한의 연계를 통해 기록을 관리하고 보존한다. 생산 기관과 아카이브 기관의 기록 정보 공유를 기반으로 한 체계이며, 블록체인 네트워크를 통해 신뢰 기반이 강화된다.

네트워크를 구성하는 노드는 일반노드와 핵심노드(Key node)로 구성된다. 앞서 제안하였듯이 핵심노드는 일반노드에서 수신된 블록의 내용정보 데이터를 블록에 저장하여 블록을 생성하는 역할을 한다. 핵심노드들은 블록 검증 위원회의 승인 과정을 거쳐 블록을 생성하고 전파한다. 일반노드는 생성된 블록을 받아 체인에 연결한다. 핵심노드 중 주체적 역할을 하는

한 노드를 정하여 주요노드(Primary node)라 하고, 이 주요노드는 블록 생성 과정을 모니터링하고, 해시 검증 요청을 수신하고 그 결과값을 조회하여 블록체인 검증서를 발행하는 역할을 한다.

이 주요노드와 핵심노드, 일반노드는 영구기록물관리기관, 기록관, 각 처리과를 의미하는 것이 아니다. 노드에 참여하는 기록관리 기관은 사전 네트워크 구성 합의 과정에서 핵심노드와 일반노드를 구성한다. 모니터링 기능과 검색(retrival) 및 제출기능을 수행하는 주요노드는 중앙기록물관리기관 혹은 네트워크에 참여하는 학회나 협회와 같이 여타 노드와는 성격을 달리하는 기관의 서버에서 담당하게 할 수도 있다. 참여하는 모든 노드에 네트워크 구성시의 합의에 의한 역할을 부여한다. 블록의 내용도 동일하며 동등한 방식으로 분산하여 저장한다. 이로써 각 노드는 수평적 체계를 갖는다고 할 수 있다. 각 기관은 노드의 역할에 따라 블록을 생성하는 노드와 생성된 블록을 수용하는 노드로 구분되기는 하지만 계층적 구조의 개념이 아닌 수평적 체계에서의 역할 분담으로 이해해야 한다. 이는 블록을 생성하고 축적하는 과정의 합의 형성에 이르기 위한 효율적인 방법을 찾기 위한 것이다.

이러한 기록관리 체계는 기존의 단계적이고 분절적인 기록관리와는 다른 패러다임으로 전환될 것이다. 기록 생산부터 아카이브 서비스까지의 통합 시스템을 활용함으로써 논리적 객체 정보의 접근 권한 통제를 통해 기록의 관할권을 관리하게 되며 정보의 공유를 통해 위변조, 의도적 폐기와 삭제로부터 기록을 보호하는 강력한 체계를 구축할 수 있다. 기관의 기록은 기관 내의 기록관리 기관에서 생산부터 아카이브서비스까지 실행하도록 하며, 중앙기록물관리기관은 내셔널아카이브로서의 기능과 정책 개발 및 연구 기능을 수행하게 된다. 이 관계는 수직적이고 계층적인 구조에서 협력적인 체계로 전환되는 것이다. 또한 각 기록물관리기관 간의 관계도 네트워크를 구성하는 수평적 노드 체계가 되는 것이다.

5. 결론

이 연구에서 제안한 기록관리 블록체인 모형은 전자기록의 진본 인증에 유의미한 이점이 있음을 확인하였고, 블록체인의 분산 저장 개념이 기록관리 체계의 수평적 구조로의 변화를 수반한다는 점을 밝혔다.

그러나 현재 블록체인 기술에 대한 인식이 과장되어 있으므로 이를 경계해야 한다는 지적도 있다. 기록의 신뢰가치를 결정하는 것은 합리적인 위험평가의 결과에 따르는 것인데, 이는 단일 기술 시스템이나 암호화 메커니즘을 넘어서는 진본인증 방안이 필요하다. 기록관리 관점에서 블록체인 적용 시 예상되는 문제점을 해소하고 그 효과를 극대화하기 위해서는 기록의 특성을 반영한 아키텍처의 설계, 법제의 정비 등이 이루어져야 할 것이다.

본 연구에서 제안한 모형 연구는 개념적 정의와 논리적 구성 방안을 제안한 것으로, 실제 기술적 구현 방법을 다루지는 못하였다. 장기적인 시각에서 전자기록관리 체계를 점검하고 재설계하는 과정에서 블록체인 기술의 효용성에 대한 연구가 진행되어야 할 것이다.

〈참고문헌〉

김석원. 2017.『블록체인 펼쳐보기』. 서울 : 비제이퍼블릭.

김익한. 2006. 전자기록의 진본 평가 시스템 모형 연구.『기록학연구』, 14, 91-117.

김한기, 김종성. 2019. 해시함수 SHA-1에 대한 공격 그리고 그 이후.『OSIA S&TR Journal』, 31(2), 10-11.

남충현. 2018. 블록체인의 다변화 : 채굴 없는 블록체인의 확산.『정보통신정책연구원 KISDI Premium Report』, 18(1), 1-16.

명지대학교 산학협력단 디지털아카이빙연구소. 2017.『차세대 기록관리 모델 재설계 연구 개발』. 대전 : 국가기록원.

설문원. 2005. 기록의 품질 기준 분석 : 진본성, 신뢰성, 무결성, 가용성을 중심으로.『기록학연구』, 11, 41-89.

아카하네 요시하루 외. 2017.『블록체인 구조와 이론』. 양현 옮김. 파주 : 위키북스.

이승억, 설문원. 2017. 전자기록관리정책의 재설계에 관한 연구.『기록학연구』, 52, 5-37.
임종철, 유현경, 곽지영, 김선미. 2018. 블록체인과 합의 알고리즘.『전자통신동향분석』, 33(1), 45-56
한국정보화진흥원. 2018. 지능형 정부 추진을 위한 블록체인 동향분석 및 시사점.『D.gov Trend & Future』, 2018(1).
CCSDS. 2012. Reference Model for an Open Archival Information System(OAIS). CCSDS 650.0-M-2. Magenta Book.
Government of Canada. 2017. Electronic records as documentary evidence. National Standard of Canada CAN/CGSB-72.34-2017(Supersedes CAN/CGSB-72.34-2005).
ISO. 2015. ISO 15489 - Information and documentation－Records management－Part1 : Concepts and principles.
ISO/TC 307 "Blockchain and distributed ledger technologies".
InterPARES 2 Project Dictionary.
InterPARES 2 Project Ontology.
Klaus Schwab. 2016. The Fourth Industrial Revolution : what it means, how to respond. World Economic Forum.
Laure A. Linn & Martha B. Koo. 2016. Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research.
Luciana Duranti. 2007. Archives as a Place.『Archives & Social Studies : A Journal of Interdisciplinary Research』, 1, 445-466.
Satoshi Nakamoto. 2009. Bitcoin : A Peer-to-Peer Electronic Cash System.
Stephen Thompson. 2017. The preservation of digital signatures on the blockchain.『The University of British Columbia iSchool Student Journal』, 3, 1-17.
The Electronic Discovery Reference Model(EDRM) LLC. 2011. How the Information Governance Reference Model (IGRM) Complements ARMA International's Generally Accepted Recordkeeping Principles (GARP®).
Victoria L. Lemieux. 2017. Blockchain and Distributed Ledgers as Trusted Recordkeeping Systems : An Archival Theoretic Evaluation Framework. Future Technologies Conference(FTC).
Victoria L. Lemieux. 2016a. Blockchain Technology for Recordkeeping, vol.1 : Report. The University of British Columbia, Vancouver.
Victoria L. Lemieux. 2016b. Blockchain Technology for Recordkeeping, vol.2 : Appendices. The University of British Columbia, Vancouver.
Victoria L. Lemieux. 2016c. Trusting records : is Blockchain technology the answer?『Records Management Journal』, 26(2), 110-139.
Vitalik Buterin. 2015. On Public and Private Blockchains. Ethereum Blog.